|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **K. SANTOSH REDDY**   |  |  |  |  | | --- | --- | --- | --- | | **Phone:** | **+91-8121835680** | **E-Mail:** | **kethirisantoshreddy71@gmail.com** | | |
| **Aspiring to leverage extensive expertise as a SOC Analyst, emphasizing cybersecurity practices, particularly in the realms of Incident Response and Threat Intelligence, to enhance organizational security measures.** | |
| |  | | --- | | **ǁ Profile Summary ǁǁǁǁǁǁ** | | * **Nearly 4 years** of hands-on experience in **incident detection, analysis, and response**, ensuring a proactive approach to IT security and risk mitigation. * Currently working as, a **SOC Analyst at iSolution**, administering **security alerts, incident response, and enterprise network protection** to strengthen organizational cybersecurity. * Skilled in **log analysis, malware remediation, and security monitoring**, leveraging tools such as **SIEM (IBM QRadar), EDR (SentinelOne), and threat intelligence platforms** to detect and neutralize threats. * Enhanced **incident response efficiency** by streamlining processes, implementing best practices, and collaborating with cross-functional teams, leading to improved SOC performance. * Possesses strong analytical skills to **identify, investigate, and mitigate security threats**, while fostering a culture of **security awareness and best practices** within teams. * Proficient in **MITRE ATT&CK, NIST, ISO 27001, and other security frameworks**, ensuring effective **threat detection, incident management, and regulatory compliance**. * Stayed up to date with **emerging cybersecurity threats, attack vectors, and vulnerabilities**, implementing **preventive strategies** to safeguard critical assets and maintain compliance. * Actively contributed to **security awareness programs**, educating users on **phishing threats, malware risks, and social engineering tactics** to strengthen overall organizational security. |  |  | | --- | | **ǁ Core Competencies ǁǁǁǁǁǁ** | | |  |  |  | | --- | --- | --- | |  |  |  | | Cybersecurity Incident Management | Threat Intelligence Analysis | Security Operations Center (SOC) | | Risk Assessment and Mitigation | Vulnerability Management | Security Policy Development | | Compliance and Regulatory | Security Awareness Training | Network Security Architecture | |  |  |  | |  |  |  | | --- | --- | | **ǁ Technical Skills ǁǁǁǁǁǁ** | | | **SIEM:** IBM QRadar  **Security Tools:** Wireshark, Nessus, Snort, OpenVAS  **Threat Intelligence:** VirusTotal  **Email Security:** Proofpoint | **EDR:** SentinelOne  **Operating Systems:** Windows, Linux  **Ticketing Tools:** ServiceNow  **Scripting:** Python, PowerShell, Bash |  |  | | --- | | **ǁ** **Work Experience ǁǁǁǁǁǁ** | | **Dec'2023 to Present: SOC Analyst at iSolution (Remote), Hyderabad**  **Role:**   * **Security Monitoring:** Engaging in continuous security monitoring using IBM QRadar to detect and respond to potential threats. * **Incident Investigation:** Investigating security incidents by analyzing Channels, Events, Annotations, and Reports to assess threat severity. * **Incident Management:** Logging and categorizing incident tickets for internal and external users, ensuring accurate tracking and resolution. * **Collaboration & SLA Compliance:** Collaborating with teams to resolve incidents within SLAs, improving operational efficiency. * **Reporting & Documentation:** Generating detailed daily, weekly, and monthly security reports aligned with client requirements. * **Threat Analysis:** Analyzing phishing attempts, spam emails, and malware threats to enhance organizational security. * **Real-Time Threat Response:** Conducting real-time monitoring, investigation, and escalation of security events for rapid response. * **Security Awareness & Research:** Supporting threat intelligence research and security awareness initiatives to educate users on recognizing threats.   **Achievements:**   * Successfully identified and mitigated a significant phishing attack, preventing potential data breaches and safeguarding sensitive information. * Developed and implemented a training program for new team members, improving onboarding efficiency and knowledge retention. * Recognized for outstanding performance in incident management, receiving commendation from management for exceptional dedication and results.   **May'2020 to Dec'2023: SOC Analyst at Cognizant, Pune**  **Role:**   * **SIEM Monitoring:** Utilized IBM QRadar SIEM to supervise security operations, ensuring continuous monitoring and effective management of security incidents across the organization. * **Log Analysis:** Performed detailed log analysis from multiple sources, including DLP systems, IDS/IPS, Antivirus solutions, firewalls, AD, DNS, and DHCP servers, to identify potential security threats. * **Malware Investigation:** Investigated malware incidents by assessing their priority, escalating them as needed, and ensuring timely remediation to prevent further impact. * **Incident Validation:** Distinguished between false positives and genuine security incidents, implemented appropriate remediation strategies to minimize risks and enhance system security. * **SIEM Reporting:** Created and maintained SIEM reports and dashboards to support continuous security monitoring, providing insights into threats, trends, and system vulnerabilities. * **Endpoint Security:** Leveraged Endpoint Detection and Response (EDR) tools for in-depth malware analysis and effective remediation to strengthen endpoint security. * **Documentation & Knowledge Sharing:** Developed and maintained documentation of security incidents and response actions, fostering knowledge sharing and continuous improvement within the SOC team. * **Security Tool Integration:** Spearheaded the integration of new security tools into existing workflow, enhancing the SOC’s skill to detect, analyze, and respond to threats in real-time.   **Achievements:**   * Played a pivotal role in the development of a centralized reporting system that improved visibility into security incidents and trends. * Recognized for exceptional teamwork and collaboration, contributing to the successful resolution of high-priority security incidents. * Contributed to the successful completion of a major security audit, ensuring compliance with industry standards and best practices. |  |  | | --- | | **ǁ Projects ǁǁǁǁǁǁ** | | **SIEM Implementation Project**   * Configured and optimized IB M QRadar SIEM to enhance alert detection, improve log correlation, and fine-tune security rules for more effective threat monitoring and response.   **Threat Hunting Exercises**   * Conducted hands-on threat hunting exercises to identify adversary tactics, techniques, and procedures (TTPs) using security frameworks like MITRE ATT&CK, improving proactive threat detection capabilities.   **Security Awareness Initiatives**   * Assisted in developing and delivering security awareness training programs to educate users on recognizing phishing attacks, malware threats, and social engineering tactics, strengthening the organization’s security posture. |  |  | | --- | | **ǁ Education ǁǁǁǁǁǁ** | | **2019:** M.Tech. in Information Technology, Charles Sturt University, Australia  **2015:** B.Tech. in Electronics and Communication, SRM University, Chennai |  |  | | --- | | **ǁ Personal Details ǁǁǁǁǁǁ** | | **Date of Birth:** 26th August 1994  **Languages Known:** English, Telugu, Hindi, Tamil  **Address:**  Hyderabad – 500019, Telangana | |